DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 14| Agosto 2021

UTILIZACIÓN DE APPS Y PRINCIPALES RIESGOS PARA LOS CIUDADANOS

ÍNDICE

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

La tecnología está cambiando la forma de trabajar de las Administraciones Públicas (en adelante, AA.PP.) y su relación con los ciudadanos buscando mejorar tiempos, facilitando la accesibilidad y simplificando trámites, no obstante, existe un riesgo específico asociado al tratamiento de datos personales por las AA.PP. al hacer uso de tecnologías emergentes. En este sentido, y respondiendo a la realidad actual hay que tener en cuenta algunas de las tecnologías en la lucha contra la COVID-19, de los beneficios que prometen frente a la pandemia y de los costes en la privacidad de los individuos.

Hay que tener en cuenta que antes de implementar soluciones tecnológicas para enfrentarnos a la COVID-19 es imprescindible que éstas se encuentren integradas en el marco de medidas jurídicas y organizativas realistas, eficaces, basadas en criterios científicos, legítimas y proporcionales. El beneficio tendrá que medirse en función de una menor propagación de la infección en términos globales, con la posibilidad de recuperar la libertad de acción, y una protección de la salud de los individuos. Los datos de salud tienen un alto valor, por lo que hay que prevenir que, aprovechando la incertidumbre que provoca una situación de emergencia, se produzcan abusos por parte de terceros que conduzcan a situaciones de pérdida de libertades.

En este boletín se va a realizar un breve análisis, con propósito didáctico de algunas de las tecnologías en la lucha contra la COVID-19, de los beneficios que prometen aportar frente a la pandemia y de los costes en la privacidad que nos pueden acarrear, en particular:

- Geolocalización mediante la información recogida por los operadores de telecomunicaciones
- Apps de recogida de información de contagiados
- Apss de seguimiento de contactos
- Pasaportes digitales de inmunidad

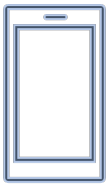
GEOLOCALIZACIÓN

Esta técnica consiste en que los operadores de telefonía móvil proporcionen información anonimizada de la ubicación de los usuarios en las celdas de telefonía que definen sus antenas. Las operadoras recogen habitualmente datos de posición de sus abonados.

Con esta información, que es necesaria para prestar el servicio, una operadora es capaz de estimar qué números de teléfono hay en cada celda en un determinado momento, e incluso dar una ubicación aproximada de cualquier teléfono móvil activo en una celda.

Esta información, sin anonimizar, puede ser demandada por las Fuerzas y Cuerpos de Seguridad siempre mediando una orden judicial. Por otro lado, su utilización anonimizada fue utilizada por el Instituto Nacional de Estadística para estudios de movilidad. Durante la gestión de la crisis de la COVID-19, el Gobierno y la Comisión Europea han pedido que las operadoras proporcionen este tipo de información anonimizada para ver los movimientos de población.

"…DURANTE LA GESTIÓN DE LA CRISIS DE LA COVID-19, EL GOBIERNO Y LA COMISIÓN EUROPEA HAN PEDIDO QUE LAS OPERADORAS PROPORCIONEN ESTE TIPO DE INFORMACIÓN ANONIMIZADA PARA VER LOS MOVIMIENTOS DE POBLACIÓN".



¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Con una gestión cuidadosa, el acceso apropiadamente anonimizado a dicha información no debería de representar una amenaza mayor que la que ya representaban antes. Es decir, siempre cabe la posibilidad de una anonimización incompleta, una subcontratación poco rigurosa o un ciberataque que pusiera en manos de un tercero la localización de los móviles de los usuarios, aunque este riesgo ya existía antes de la pandemia.

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

Conocer los patrones de movilidad de la población, ver dónde se desplazan las personas cuando trabajan o los fines de semana, puede ser beneficioso para una administración en cualquier tiempo.

Ahora bien, hay que evaluar de forma continua su utilidad frente a los escenarios cambiantes de una situación de confinamiento global o parcial. Una derivada que se ha apuntado es la posibilidad de que se usaran datos anonimizados de geolocalización para observar movimientos globales, pero con la posibilidad de que la policía pidiera la reidentificación en determinados casos conforme a los criterios establecidos por las autoridades sanitarias para garantizar el control de la epidemia.

APPS DE INFORMACIÓN VOLUNTARIA DE CONTAGIOS

En esta categoría estarían algunas aplicaciones móviles que surgieron de forma casi instantánea, en algunos casos de iniciativas ciudadanas, y que pretendían hacer sus propios mapas y estadísticas de propagación de la COVID-19 a partir de datos proporcionados voluntariamente por nosotros como usuarios. En un entorno muy abierto y transparente se apela a la colaboración desinteresada para descargarse estas aplicaciones y subir datos de localización y datos de su posible infección, contribuyendo así a hacer mapas y cuadros de mando con una información que teóricamente no está filtrada por las autoridades

¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Estas Apps podrían serlo si los fines que declaran no son tan altruistas como los que promueven o las prisas conducen a desarrollos sin garantías para la privacidad. No olvidemos que lo que se está cediendo a los servidores en Internet son datos de salud y localizaciones precisas.

Si la cantidad y calidad de estos datos fuera la suficiente, gracias a un número significativo de usuarios, se dispondrían de conclusiones como barrios con alto nivel de infección, con el estigma social que eso puede acarrear. Es decir, es necesario disponer de una muestra significativa y que nadie, de forma maliciosa, esté proporcionando información falsa o manipulada para beneficiar o perjudicar al conjunto.

"…ESTAS APPS PODRÍAN SERLO SI LOS FINES QUE DECLARAN NO SON TAN ALTRUISTAS COMO LOS QUE PROMUEVEN O LAS PRISAS CONDUCEN A DESARROLLOS SIN GARANTÍAS PARA LA PRIVACIDAD. NO OLVIDEMOS QUE LO QUE SE ESTÁ CEDIENDO A LOS SERVIDORES EN INTERNET SON DATOS DE SALUD Y LOCALIZACIONES PRECISAS".

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

Desde el principio del uso voluntario y descontrolado no es posible saber nunca la fiabilidad de la información que contienen, por lo que pueden contribuir a divulgar noticias erróneas y resultar un perjuicio.

APPS DE SEGUIMIENTO DE CONTACTOS POR BLUETOOTH

Este tipo de aplicaciones usa la tecnología bluetooth de los teléfonos móviles que permite la conexión con aparatos cercanos como auriculares, altavoces o relojes.

En este caso, las apps utilizan el bluetooth para enviar la "tarjeta" correspondiente al usuario con los móviles que se va encontrando en su camino, y a la vez recolecta las "tarjetas" de esos mismos móviles. Cada tarjeta no tiene una identificación real del usuario, sino un apodo de su identidad. De esta manera cada móvil tiene una colección anónima de "tarjetas" de la gente con la que ha estado en su trabajo, en el transporte o en su ocio. Si un determinado usuario averigua que está infectado, tiene en su mano la posibilidad de "declararlo" a través de la app a un servidor central. En ese momento, se supone que aquellas personas que con las que estuvo en contacto en los últimos días, recibirán un aviso para que valoren qué acciones tomar, como podría ser confinarse, contactar con sus servicios sanitarios o realizarse una prueba.

Han surgido varias estrategias para implementar esta tecnología, existen opciones en las que ese control descansa en el propio usuario (descentralizadas), y otras en un control centralizado, supuestamente por una autoridad.

¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Las principales amenazas a la privacidad de este tipo de soluciones vienen de la realización de mapas de relaciones entre personas, reidentificación por localización implícita, de la fragilidad de los protocolos a la hora construir "tarjetas" casi anónimas, y de dispersar las señales de los contagios de forma que no se identifique en ningún caso la identidad de los contagiados. Debe tenerse en cuenta que el tratamiento de la información no solo afecta al usuario de la aplicación sino también la de todos los terceros con los que ha estado en contacto, por lo que este tratamiento ha de cumplir los principios de protección de datos. La posibilidad de que, debido a la acumulación de los datos de forma centralizada, se produjese un abuso en una empresa poco ética, se ampliarán los propósitos del tratamiento o se fuera víctima de un ciberataque constituye otra de las mayores amenazas de este tipo de soluciones.

¿REPRESENTAN ESTOS DATOS EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

Es preciso poner de manifiesto que las soluciones técnicas no se pueden considerar de forma aislada. En primer lugar, es necesaria la implicación de un elevado número de usuarios, algunos estudios hablan de al menos el 60% de una población. Por otro lado, depende de que se realice una declaración responsable de la situación personal de infección, preferiblemente supervisada por un profesional para evitar estrategias de desinformación. Finalmente, es necesario disponer de acceso a test, no solo para todos los usuarios, sino para poder actualizar la información periódicamente y para que aquellos que sean notificados de haber estado en contacto con un infectado puedan realizar la prueba con prontitud.

En la situación actual de España y de otros países europeos, no parece que estas aplicaciones vayan a tener éxito a corto plazo como una estrategia global de lucha contra la pandemia, más aún si tenemos en cuenta el crecimiento de personas vacunadas. Si pensamos en un escenario futuro, cuando la enfermedad esté mucho más controlada, sí podría tener su éxito en colectivos concretos como estudiantes de un centro, profesionales de una compañía o grupos de amigos que deciden voluntariamente usar la aplicación.

PASAPORTES DE INMUNIDAD

Han empezado a considerarse el uso de Apps equivalentes a lo que sería un pasaporte o salvoconducto en papel, mostrando un código de colores o un código QR, para que un vigilante o un sistema de control de acceso pueda dejar pasar o no al portador, como podrían ser las tarjetas de embarque de los vuelos.

¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UNA AMENAZA A LA PRIVACIDAD?

Estas aplicaciones están valiéndose de un documento de identidad en el móvil, con el riesgo añadido de incluir y mostrar un dato de salud, e incluyendo los riesgos de dichos sistemas: acceso a manos de ciberdelincuentes, cruce con otros datos como la localización, incorporación de metadatos, o simplemente no estar al alcance de muchas personas que no pueden usar teléfonos inteligentes. A diferencia de una tarjeta de embarque, las pruebas para determinar si una persona está sufriendo o ha superado la enfermedad deberían ser presenciales, y el personal podría proporcionar al usuario un certificado o cualquier soporte de baja tecnología para que lo mostrara cuando le fuera requerido. Un sistema de identidad móvil solo puede tener ventajas cuando el alta se puede hacer a distancia o si la información que gestiona cambia rápidamente.

¿REPRESENTAN ESTAS APLICACIONES EN LA CRISIS DE LA PANDEMIA UN BENEFICIO IMPORTANTE?

El pasaporte de inmunidad incorpora un dato sensible, como es cualquier dato de salud, pero al que también se le ha dado la misión de servir como salvoconducto de acceso. Un uso bien gestionado de Apps para certificaciones o registros de salud, que los mantuviera actualizados, seguros e interoperables tendrá cierta utilidad en ámbitos concretos siempre que el acceso a dicha información sea realizado por personal vinculado al cumplimiento de las finalidades relacionadas con políticas públicas para el control de la pandemia. Sin embargo, como en todas las aplicaciones que requieren el uso de smartphones y la evidencia de una prueba fiable de infección o de anticuerpos, se está lejos de alcanzar a una totalidad de la población. No hay que olvidar, que no solo se está recurriendo al uso de estas Apps, sino también al uso del papel, donde sea mas accesible y menos invasivo para la privacidad que el uso de las tecnologías.

"…UN USO BIEN GESTIONADO DE APPS PARA CERTIFICACIONES O REGISTROS DE SALUD, QUE LOS MANTUVIERA ACTUALIZADOS, SEGUROS E INTEROPERABLES TENDRÁ CIERTA UTILIDAD EN ÁMBITOS CONCRETOS SIEMPRE QUE EL ACCESO A DICHA INFORMACIÓN SEA REALIZADO POR PERSONAL VINCULADO AL CUMPLIMIENTO DE LAS FINALIDADES RELACIONADAS CON POLÍTICAS PÚBLICAS PARA EL CONTROL DE LA PANDEMIA. SIN EMBARGO, COMO EN TODAS LAS APLICACIONES QUE REQUIEREN EL USO DE SMARTPHONES Y LA EVIDENCIA DE UNA PRUEBA FIABLE DE INFECCIÓN O DE ANTICUERPOS, SE ESTA LEJOS DE ALCANZAR A UNA TOTALIDAD DE LA POBLACIÓN."

RECOMENDACIONES A TENER EN CUENTA

En caso de que se decidiera optar por su uso, se deberían evitar los riesgos anteriormente señalados, y es importante para ello tener en cuenta las siguientes recomendaciones;

¿QUÉ PUEDEN HACER LOS USUARIOS PARA EVITAR LOS RIESGOS?

La finalidad debe estar claramente definida y debe limitarse a la gestión de medidas de distancia social, control de vacunados o de contagios, tales como el control de aforo o el control de distancia.

Los tratamientos que se propongan han de ser realmente efectivos con relación a la finalidad y no pueden generar falsas expectativas de seguridad de acuerdo con el principio de lealtad del tratamiento. Deben quedar claras las finalidades concretas que se persiguen, no mezclando funcionalidades como fidelización, publicidad o redes sociales.

La implementación de tratamientos basados en Apps deberá fundamentarse en un análisis de necesidad y proporcionalidad que determine tanto la utilización de la App como el conjunto de datos mínimo necesario para conseguir los fines que se persiguen. En particular, la identidad del usuario o su seguimiento, incluido el uso de identificadores únicos de cualquier tipo o aquellos procedentes del bluetooth, solo podrá tratarse si son estrictamente necesarios para la finalidad de la App, tal como se ha abordado anteriormente en el boletín.

No se deberán tratar categorías especiales de datos, en particular datos de salud, teniendo en cuenta la finalidad perseguida y la anonimización de los mismos, y , en su caso, los estrictamente necesarios para gestionar los espacios reservados a personas con discapacidad.

El uso de una App debe ser de carácter voluntario, basado en el consentimiento para el tratamiento de los datos personales necesarios para cada una de las funcionalidades que se persiguen. El tratamiento deberá estar basado en un consentimiento libre, informado y específico.

El tratamiento de datos personales de menores de 14 años por este tipo de Apps debe ser consentido por sus padres o tutores.

MATERIAL COMPLEMENTARIO

- La AEPD publica unas directrices orientadas a aplicaciones móviles educativas y de actividad física, bienestar y salud. Consulta en este enlace.
- La AEPD publica un informe sobre los tratamientos de datos en relación con el COVID-19. Consulta el documento en este enlace.
- La AEPD elabora unas recomendaciones para el despliegue de aplicaciones móviles en el acceso a espacios públicos. Consulta las recomendaciones en este enlace.
- La AEPD elabora una guía de privacidad y seguridad en Internet. Consulta este enlace para ver la guía.
- La AEPD elaboró una Nota Técnica sobre el deber de informar y otras medidas de responsabilidad proactiva en Apps para dispositivos móviles. Consulta las recomendaciones en este enlace.

NOTICIAS

- **La compañía de distribución Mercadona abonará 2,5 millones de euros de sanción propuesta por la Agencia Española de Protección de Datos (AEPD) como penalización por un proyecto piloto que la compañía testó en algunas tiendas y que permitía detectar personas con orden de alejamiento de sus establecimientos.** Así Mercadona anuncia en un comunicado, que "ha decidido dar por finalizado el procedimiento abierto por la AEPD en relación con el proyecto piloto que fue testado durante varios meses en 48 de las 1.640 tiendas de las que dispone la compañía", vistas la "indefinición y dudas legales sobre el sistema de detección anticipada que la compañía implantó a modo de prueba piloto". Consulta el artículo en **este enlace.**

- **La AEPD publica una nueva guía para gestionar el riesgo de los tratamientos de datos personales y realizar evaluaciones de impacto**. La Agencia Española de Protección de Datos (AEPD) ha presentado hoy la guía '**Gestión del riesgo y evaluación de impacto en tratamientos de datos personales**', un documento que incorpora la experiencia acumulada en la aplicación de la gestión del riesgo en el ámbito de la protección de datos desde la aplicación del Reglamento General de Protección de Datos (RGPD) y añade las interpretaciones de la AEPD, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos. El documento, **dirigido a personas responsables, encargadas de tratamientos y personas delegadas de protección de datos (DPD)**, ofrece una visión unificada de la gestión de riesgos y de las evaluaciones de impacto en protección de datos, y facilita la integración de la gestión de riesgos en los procesos de gestión y gobernanza de las entidades. Consulta el artículo en este enlace.